Cryptography Sheet 3 2
Answers

$2 \cdot \frac{1}{2} = 2 \cdot \frac{1}{2} = 1$

1) From a theoretical point of view, PKCS can be used as a replacement for symmetric cryptography.
However, in practical applications, symmetric ciphers tend to approx 1000 times faster than public key schemes. Hence, symmetric ciphers are used when it comes to bulk data encryption

2) Every pair out of $n = 120$ employees requires a distinct key

$$n \cdot \frac{(n-1)}{2} = 120 \cdot \frac{(120-1)}{2} = 7140$$

3) gcd(7469, 2464)

$$7469 = 2464(3) + 77$$
$$2464 = 77(32) + 0$$

$$\gcd(7469, 2464) = 77$$

ced

b) gcd(2689, 4001)

$4001 = 2689(1) + 1312$

$2689 = 1312(2) + 65$

$1312 = 65(20) + 12$

$65 = 12(5) + 5$

$12 = 5(2) + 2$

$5 = 2(2) + 1$

$2 = 1(2) + 0$

$\gcd(2689, 4001) = 1$

4) gcd(198, 243)

$243 = 198(1) + 45$

$198 = 45(4) + 18$

$45 = 18(2) + 9$

$18 = 9(2) + 0$

$9 = 45 - 18(2)$

$= 45 - 2(198 - 4(45))$

$= 9(45) - 2(198)$

$= 9(243 - 198) - 2(198)$

$= 9(243) - 11(198)$

$s = 9 \quad t = -11$

b) $\gcd(1819, 3587)$

$3587 = 1819(1) + 1768$

~~$1768 =$~~

$1819 = 1768(1) + 51$

$1768 = 51(34) + 34$ ✓

$51 = 34(1) + 17$ ✓

$34 = 17(2) + 0$

~~$17 = 51 - 34$~~

~~$= 51 - (1768 - 51(34))$~~ ✓

~~$= 35(51) - 1768$~~

~~$= 35(1819 - 1768) - 1768$~~

~~$= 35(1819) - 36(1718)$~~

$$
\begin{aligned}
17 &= 51 - 34 \\
&= 51 - (1768 - 51(34)) \\
&= 35(51) - 1768 \\
&= 35(1819 - 1768) - 1768 \\
&= 35(1819) - 36(1768) \\
&= 35(1819) - 36(3587 - 1819) \\
&= 71(1819) - 36(3587)
\end{aligned}
$$

$s = 71 \quad t = -36$

5) $7x \equiv 1 \mod 26$

gcd

$26 = 7(3) + 5$

$7 = 5(1) + 2$

$5 = 2(2) + 1$

$2 = 1(2) + 0$

$1 = 5 - 2(2)$

$= 5 - 2(7 - 5)$

$= 3(5) - 2(7)$

$= 3(26 - 7(3)) - 2(7)$

$= 3(26) - 11(7)$

$7x - 26y = 1$

$7(-11) - 26(-3)$

$x = -11$ or $x = 15$

b) $19x \equiv 1 \mod 999$

$999 = 19(52) + 11$

$19 = 11(1) + 8$

$11 = 8(1) + 3$

$8 = 3(2) + 2$

$3 = 2(1) + 1$

$2 = 1(2) + 0$

$1 = 3 - 2$

$1 = 3 - (8 - 3(2))$

$= 3(3) - 8$

$= 3(11 - 8) - 8$

$= 3(11) - 4(8)$

$= 3(11) - 4(19 - 11)$

$= 7(11) - 4(19)$

$\cancel{= 7(999 - 19(52)) - 4(19)}$

$\cancel{= -437(19) + 7(999)}$

$= 7(999 - 19(52)) - 4(19))$

$= 7(999) - 368(19)$

$a = -368$

$a = 631$

5) $\phi(12) = 4$

$\phi(15) = \phi(3 \cdot 5) = \phi(3-1)\phi(5-1)$
$= 2 \cdot 4 = 8$

$\phi(26) = \phi(2 \cdot 13) = 1 \cdot 12 = 12$

Scanned by CamScanner

7) $a = 4$ and $n = 7$

$4x \equiv 1 \bmod 7$

Trial and error gives. $x = 2$

b) $a = 5$ and $n = 12$

$5x \equiv 1 \bmod 12$

$12 = 5(2) + 2$

$5 = 2(2) + 1$

$2 = 1(2) + 0$

$1 = 5 - 2(2)$

$= 5 - 2(12 - 5(2))$

$= 5(5) - 2(12)$

$a^{-1} = 5$

c) $a = 6$ $n = 13$

$6x \equiv 1 \bmod 13$

$13 = 6(2) + 1$

$6 = 1(6) + 0$

$1 = 13 - 6(2)$

$1 = a \cdot 6(-2) + 13(1)$

$a^{-1} = 11$

a) $\phi(6) = \phi(3 \cdot 2) = (3-1)(2-1)$
$= 2$

$a^2 \equiv 1 \bmod 6$ if $\gcd(a, 6) = 1$

$a = 1, 5, 0$

$0 \equiv 0 \bmod 6$

$1^2 \equiv 1 \bmod 6$ $\quad 2^2 \equiv 4 \bmod 6$

$5^2 \equiv 1 \bmod 6$ $\quad 3^2 \equiv 3 \bmod 6$

1, 2, 4, 5
7, 8

b) $\phi(9) = \phi(3 \cdot 3) = \cancel{(3-1)(3-1)}$ $\quad 3^2 - 3^1 = 6$
$= \cancel{4}$

$a^6 \equiv 1 \bmod 9$ if $\gcd(a, 9) = 1$

$1^6 \equiv 1 \bmod 9$ $\quad 4^6 \equiv 1 \bmod 9$ $\quad 8^6 \equiv 1 \bmod$

$2^6 \equiv 1 \bmod 9$ $\quad 5^6 \equiv 1 \bmod 9$

$3^6 \equiv 0 \bmod 9$ $\quad 6^6 \equiv 0 \bmod 9$

$7^6 \equiv 1 \bmod 9$

9) $p = 41 \quad q = 17$

$\phi(n) = (p-1)(q-1)$

$= 40 \cdot 16 = 640$

$\gcd(e, \phi(n)) = 1$

$e_2 = 49$ or $e_1 = 31$ both valid

$K_{pub} = (n, e) = (640, 49)$

$d = e^{-1} \bmod \phi(n)$

$= 49^{-1} \bmod 640$

$640 = 49(13) + 3$

$49 = 3(16) + 1$

$3 = 1(3) + 0$

$1 = 49 - 3(16)$

$= 49 - 16(640 - 49(13))$

$= -16(640) + 209(49)$

$d = 209$

$K_{pr} = 209$

4) $2 \cdot 2^{1001110} = 2^{1001111}$ MUL

$2^2 = 4$

$4^2 = 16$

$(16)^2 = 256$

$256 \cdot 2 = 512$

$7^2 = 49$

$49 \cdot 2 = 98$

$(98)^2 = 9$

$9 \cdot 2 = 18$

$18^2 = 324$

$324 \cdot 2 = 648$

42

Scanned by CamScanner

b) $x=3 \quad e=197 \quad m=101$

$3^{197} \bmod 101$

$3^{11000101} \bmod 101$

$(3^{1})^2 = 3^{10}$ Square $3^2 = 9$

$(3^{10}) \cdot 3 = 3^{11}$ MUL $9 \cdot 3 = 27$

$(3^{11})^2 = 3^{110}$ Square $(27)^2 = 729$

$(3^{110})^2 = 3^{1100}$ Square $(22)^2 = 484$

$(3^{1100})^2 = 3^{11000}$ Square $(80)^2 = 37$

$(3^{11000})^2 = 3^{110000}$ Square $(37)^2 = 56$

$(3^{11000}) \cdot 3 = 3^{110001}$ MUL $56 \cdot 3 = 108$

$(3^{110001})^2 = 3^{1100010}$ Square $(67)^2 = 45$

$(3^{1100010})^2 = 3^{11000100}$ Square $(45)^2 = 5$

$(3^{11000100})^2 \cdot 3 = 3^{11000101}$ MUL $5 \cdot 3 = 15$

Scanned by CamScanner

11) $p = 3 \quad q = 11 \quad d = 7 \quad x = 5$

$n = pq = 3 \cdot 11 = 33$

$\phi(n) = (p-1)(q-1) = 2 \cdot 10 = 20$

$\gcd(e, 20) = 1$ ~~choose e=3~~

Must find e, since $d = 7$ we have

$7e \equiv 1 \bmod 20$, clear $e = 3$

encryption :- $y = x^e \bmod n$

$y = 5^3 \bmod 33$

$y = 26$

b) $p = 5 \quad q = 11 \quad e = 3 , \quad x = 9$

$n = 5 \cdot 11 = 55$

$\phi(n) = (p-1)(q-1) = 4 \cdot 10 = 40$

$\gcd(e, 40) = 1$

Must find d, since $d = 3$

$3d \equiv 1 \bmod 40$

$40 = \cancel{13(3)+}\ 3(13) + 1$

$3 = 1(3) + 0$

$1 = 40 - 3(13)$

$1 = 13(-3) - 40(-1)$

$d = -13$, $d = 27$

encryption :- $y = x^e \bmod n$

$= 9^3 \bmod \cancel{40}\ 55$

$= 14$

b)

12) BF attack on all possible exponents would be easily feasible.